IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, v. ANTHONY LAURITA, Defendant.	**8:13CR107** **MEMORANDUM AND ORDER**

This matter is before the court on the defendant's motion to reconsider, Filing No. 552, a ruling on a motion to suppress with respect to a Network Investigative Technique ("NIT") warrant issued in this case, Filing No. 294.[1] This is a child pornography prosecution.[2]

[1] Also pending is the defendant's objection to the government's withdrawal of a stipulation on standing, Filing No. 558. The stipulation provides:

> For the limited purpose of certain pending motions to suppress resulting from the court/warrant authorized deployment of a network investigative technique (NIT), the parties agree and stipulate as follows:
>
> 1. The court may assume that the court/warrant authorized deployment of the pertinent network investigative technique effected a Fourth Amendment search on an activating computer;
>
> 2. At the time the NIT effected a search, each defendant owned an activating computer which was located in the Defendant's residence;
>
> 3. The Government will not object to a defendant's claim of standing under the Fourth Amendment to challenge the execution of the pertinent NIT warrant;
>
> 4. Standing, as used in this stipulation, is understood and agreed to be a defendant's claim to a reasonable expectation of privacy in an area searched. The parties do not stipulate and agree regarding the question of whether any defendant has/had a reasonable expectation of privacy in the information collected pursuant to use of the NIT.

United States v. Cottom, No. 8:13-cr-108, Filing No. 117, Stipulation; *see* Filing No. 201, Order adopting stipulation. The stipulation expressly states that it was limited to the suppression motion then

I. PROCEDURAL HISTORY

Earlier in this action, Laurita and other defendants this case and the related cases of *United States v. Pierce*, *et al.*, 8:13CR106, and *United States v. Cottom, et al.* 8:13CR108, had moved to suppress evidence with respect to the NIT activating warrant and the search of their residences and computers, contending that the government failed to comply with Rule 41 in the execution of the warrant authorizing the NIT. *See, e.g.*, Filing No. 196.[3] On July 28, 2014, following a two-day evidentiary hearing on issues relating to the NIT warrant, the magistrate judge issued an R&R recommending denial of the motion to suppress. Filing No. 254. Defendant Laurita filed an objection to the R&R on the NIT warrant issue. Filing No. 259. This court overruled Laurita's objections, adopted the magistrate's findings, and denied Laurita's motion to suppress.

---

pending before the court. The defendant raises new arguments in his motion for reconsideration. The court finds the stipulation was not made in contemplation of those arguments, and the government should not be held to the representations in the stipulation. Accordingly, the defendant's objection will be overruled.

[2] The record shows "Website A" was a child pornography bulletin board which advertised and distributed child pornography together with a discussion of matters pertinent to the sexual abuse of children. *See* Filing No. 254, R&R at 5. Once installed on Website A, each time a user accessed any page of Website A, the NIT sent one or more communications to the user's computer which caused the receiving computer to deliver data to a computer controlled by the FBI which would help identify the computer which was accessing Website A. *Id.* at 6. As a result, the FBI was able to identify a computer's actual IP address and the date and time Website A was accessed together with a date and time of accession with a unique session identifier to distinguish the accession. *Id.*

[3] In a separate motion, Laurita moved to suppress a statement made to law enforcement officers, contending the statement was made in an un-Mirandized custodial interrogation. Filing No. 193. This court sustained Laurita's objection to the magistrate judge's recommendation to deny the motion to suppress. Filing No. 295, R&R; Filing No. 349, Memorandum and Order. On interlocutory appeal, that decision was reversed by the Eighth Circuit Court of Appeals. Filing No. 358, Notice of Appeal; Filing No. 550, Eighth Circuit Opinion.

Filing No. 259. This court's ruling on the NIT warrant issue was eventually appealed by defendant Joshua Welch, who was convicted of receiving and accessing child pornography after a trial. *See United States v. Pierce, et al.*, No. 8:13CR106, Filing No. 399, Notice of Appeal.[4] The Eighth Circuit assumed, without deciding, that Fed. R. Civ. P. 41 applied to the NIT warrant. *See United States v. Welch*, 811 F.3d 275, 282 (8th Cir. 2016). Although the Eighth Circuit found the government had failed to provide the requisite notice under Fed. R. Crim. P. 41(c), the court found the defendant was not entitled to suppression because there had been no showing of reckless disregard for procedure or of prejudice to the defendant. *Id.* at 281.

The Eighth Circuit affirmed this court in all respects. *Id.* at 282.

As noted *supra* at 2 n.3, the government had pursued an interlocutory appeal of this court's suppression of Laurita's statement. Filing No. 358. This court's finding that the defendant was in custody at the time he made the statement was reversed by the Eighth Circuit Court of Appeals ("Eighth Circuit") and the action was remanded for proceedings consistent with its opinion. Filing No. 550, Eighth Circuit Opinion.

On remand, the defendant moved for reconsideration of the court's earlier ruling on the propriety of the execution of the NIT warrant. *See* Filing No. 254, Report and Recommendation ("R&R"); Filing No. 294, Memorandum and Order (adopting R&R).

[4] Co-defendant Michael Huyck has also appealed and that action is presently pending at the Eighth Circuit. *See United States v. Huyck*, No. 8:13CR107, *appeal docketed,* No. 15-3649 (8th Cir. Nov. 19, 2016). Similarly, an appeal is pending in *United States v. Cottom*, No. 8:13CR108, No. 15CR239, appeal docketed, No. 16-1050 (8th Cir. Jan. 7, 2016).

The defendant now contends that the NIT warrant was void *ab ignitio* because it was issued by the United States magistrate judge without jurisdiction and without authority. Filing No. 552. He relies on the recent case of *United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016), in which the court held that because Rule 41(b) "did not grant [the magistrate] authority to issue the NIT warrant . . . [she] was without jurisdiction to do so." *Id.* at *8. The finding that the magistrate judge lacked authority to issue the warrant was based on the court's finding that "the actual property to be searched was not the NIT nor the server on which it was located, but rather the users' computers[,]" which were located outside the magistrate judge's district. *Id.* at *6.

The government resists the motion. *See* Filing No. 555. The government first argues that the defendant presents no new facts, controlling law, or any other reason why he could not have raised this issue in his initial motion to suppress. It argues that the motion should be denied on the merits because the NIT warrant was properly issued under Fed. R. Crim. P. 41 and the Federal Magistrates Act, 28 U.S.C. § 636. Further, it argues that even if the NIT warrant were found to be a technical violation of Fed. R. Crim. P. 41, suppression is not an appropriate remedy.

The court held a hearing on the present motion on May 24, 2016. At the hearing, the court offered in evidence Exhibit 101, which is an Order Authorizing Interception of Electronic Communications. *See* Filing No. 557, Court Exhibit List, Court Ex. 101, *In The Matter of the Application of the United States of America for an Order Authorizing the Interception of Electronic Communications*, No. 12WT10, Filing No. 3 (D. Neb. Oct.

26, 2012 – Nov. 18, 2012)(sealed). The court took judicial notice of Exhibits 2, 28, and 29 from the April 17, 2014 –April 18, 2014,[5] hearing as well as the stipulation (Filing No. 117 in 8:13cr108, as adopted in Filing No. 201 herein). The court kept the record open until May 31, 2016, for the government to submit responsive exhibits. Filing No. 556, text minute entry. The government submitted the Declaration of Steven A. Smith, Jr., which shows that website data indicates that the user of IP address 108.32.11.73 used a proxy service known as "tortoweb" as a bridge to access the Tor network in order to access the Pedo board hidden service website. Filing No. 561-1, Declaration of Supervisory Special Agent Steven A. Smith at 2.

II. FACTS

The facts of this and related cases are recited in the magistrate judge's R&R and the court's earlier orders and need not be repeated herein. *See, e.g.,* Filing No. 254, R&R; Filing No. 294, Memorandum and Order; *see also United States v. Cottom*, No. 8:13CR108, Filing No. 271, Memorandum and Order at 1-12. Briefly, in November of 2012, the FBI seized three Tor-network-based[6] child pornography websites that were administered by Aaron McGrath via his home and workplace in Omaha, Nebraska. The

[5] Ex. 2 is the NIT Search Warrant, Affidavit and Return, *USA v. http://jkpos24pl2r3urlw.onion,* No. 12-mj-356; Ex. 28 is Residential Search Warrant, Affidavit and Return, Anthony Laurita; and Ex. 29 is Forensic examination report, Anthony Laurita.

[6] Software known as "Tor," an acronym for "the onion router," conceals the IP addresses of people who visit certain websites, enabling them to use illicit websites without being identified by traditional law enforcement investigative methods. *See United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016).

FBI moved the computers and websites to an FBI facility in Omaha and operated them for a brief period of time during November and December of 2012 in order to conduct court-authorized monitoring of user communications pursuant to a Title III Interception order and to deploy a court-authorized NIT to obtain IP address information about users of the websites.

Several orders were entered by Chief Judge Laurie Smith Camp in connection with these cases. *See* Court Ex. 101. In an order dated October 26, 2012, the court found probable cause to believe that named interceptee Aaron McGrath was committing federal child exploitation felonies and that an electronic keystroke recording device recording the keystrokes from computers accessible to McGrath at his home in Omaha Nebraska would allow law enforcement to obtain the passwords and pass-phrases necessary to access McGrath's computers and the electronic files stored on those computers and to access communications between McGrath and others currently unknown to law enforcement. Ex. 101, Order Authorizing the Surreptitious Installation of Electronic Keyboard Keystroke and Computer Screen Capture Recording Devices to Collect Computer Keyboard Keystrokes and Computer Screen Captures at 1-2. The order authorized the collection of that information. *Id.* at 4. In an order dated November 9, 2012, the court found probable cause to believe that target subjects would use private message functions of the website in furtherance of the child exploitation offenses at issue and authorized the interception of those communications. *Id.* at 2. In another order, the court found probable cause to believe that unidentified users of a certain child

pornography website "have committed, are committing, and will continue to commit federal felony [child exploitation] offenses" and would use private message function and closed group postings of the website in furtherance of those offenses. *Id.*, Order dated Nov. 18, 2012, at 1-2. It authorized "the FBI, local law enforcement, and or individuals employed by or operating under a contract with the government and acting under the supervision of the FBI," to "intercept electronic communications of the target subjects occurring over the target facility until such electronic communications are intercepted that fully reveal:" *inter alia*, the identity of the target subjects or information that may be useful in establishing their identity. *Id.* at 4.

Pursuant to court authorization, a NIT was installed on Website A during the period of November 16, 2012, and December 2, 2012. *See* Filing No. 254, R&R at 6. The technique used in this case involved a flash application to identify the activating computer URL. *See United States v. Cottom*, No. 8:13CR108, Filing No. 271, Memorandum and Order at 5. The Flash application functioned to ignore the proxy settings of the activating computer—it would not route the connection through Tor, but it would go directly out of the user's IP address to wherever it was trying to connect. *Id.* The NIT warrant pertaining to Laurita and other users of the Pedoboard child pornography website was authorized by United States Magistrate Judge F.A. Gossett, III on November 15, 2012. Ex. 2.

Thereafter, the NIT identified the true IP addresses of Laurita and others, who were subsequently identified after residential searches and charged in the District of

Nebraska with receiving and accessing with intent to view child pornography. *See, e.g.*, Filing No. 114, Notice: Summary for Superseding Indictment (Sealed).

III. LAW

The Fourth Amendment protects individuals from "unreasonable searches and seizures" by the government. U.S. Const. amend. IV. For a search to be reasonable, the government generally must obtain a warrant supported by probable cause before "physically intruding on constitutionally protected areas" or otherwise searching areas or items in which an individual has a reasonable expectation of privacy. *Florida v. Jardines*, 569 U.S. ——, ——, 133 S. Ct. 1409, 1417 (2013). The defendant has the burden of proving a reasonable expectation of privacy in the area searched. *Rakas v. Illinois*, 439 U.S. 128, 130–31 n. 1 (1978). It is well established that there is no expectation of privacy when an individual sends information to a third party, even where that information is understood to be confidential. *See Katz v. United States*, 389 U.S. 347, 363 (White, J., concurring) ("When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates."); *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979) (finding no right to privacy in dialed telephone numbers therefore, the installation

and use of a pen register to capture the dialed phone numbers does not constitute a search.)[7]

Generally, one has no reasonable expectation of privacy in an IP address when using the Internet. *See, e.g., United States v. Forrester*, 512 F.3d 500, 509–11 (8th Cir. 1999) (noting that the lack of a reasonable expectation of privacy stems from the fact that Internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."). Surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account "are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." *Id.* at 510. Because an individual has "no reasonable expectation of privacy in his IP address" he or she "cannot establish a Fourth Amendment violation." *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (citations omitted). "[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [internet service providers]." *Id.*; *see also In re Nickelodeon Consumer Privacy Litig.*,

[7] A pen register record only the numbers called, not conversations, but can be used, in conjunction with other information, to demonstrate probable cause for electronic surveillance or a search warrant. *See e.g. Fairchild*, 189 F.3d at 776 (pen register information combined with other evidence demonstrated probable cause); *United States v. Milton,* 153 F.3d 891, 894–95 (8th Cir.1998) (same). As these authorities make clear, probable cause may be found in evidence that phone calls are made between persons thought to be engaged in criminal activity, without knowing what was said by whom during the conversation.

No. 12-cv-07829, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) ("Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers, which can be warrantlessly captured via pen registers.") (citation and internal quotation marks omitted); *Forrester*, 512 F.3d at 509–10 (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register). "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Christie*, 624 F.3d. at 574 (citations and internal quotation marks omitted).

Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address. *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016). Also, any subjective expectation of privacy is not objectively reasonable in light of the way the Tor network operates. *Id.* (noting that even a justifiable expectation of privacy is not one that society recognizes as legitimate given its unauthorized nature); *see United States v. Stanley*, 753 F.3d 114, 119 (3d Cir. 2014) (finding no legitimate expectation of privacy in accessing neighbor's wireless internet connection); *United States v. Farrell*, No. CR15–029, 2016 WL 705197, at *1 (W.D. Wash. Feb. 23, 2016) (wherein researchers operating the Tor nodes observed the IP address of the alleged

operator of Silk Road 2.0, a Tor hidden service and, pursuant to a subpoena, turned over the information to law enforcement).

Several courts have denied suppression motions involving NIT warrants in child pornography prosecutions. *See, e.g., United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016) (specifically considering the ruling and rationale of *Levin*); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (same); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (same); *United States v. Epich*, No. 15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Only one court has followed *Levin's* reasoning and suppressed evidence from that warrant. *See United States v. Arterbury*, 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. Apr. 25, 2016) (R&R); *Id.*, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016) (summarily adopting R&R). Those courts finding that a magistrate judge in one state lacks authority under Rule 41 to issue a warrant in another state, generally do not find that suppression is required or even appropriate. *Werdene*, No. 2:15-cr-00434, 2016 WL 3002376; *compare Michaud*, 2016 WL 337263, at *6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), and *Epich*, 2016 WL 953269, at *2 (rejecting Defendant's contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 2016 WL 2596010, at *7–15

(finding suppression warranted because Rule 41 "implicates substantive judicial authority," defendant was prejudiced even if the violation was technical, and the good faith exception to the exclusionary rule is not available because the warrant was void *ab initio*), and *Arterbury*, 2016 U.S. Dist. LEXIS 67091 (same).

A Title III intercept authorization is similar to an application for a warrant, and should be reviewed under the same standards. *See United States v. Fairchild*, 189 F.3d 769, 775 (8th Cir. 1999)(noting that the statutory probable cause standards of Title III are co-extensive with the constitutional requirements of probable cause under the Fourth Amendment); *United States v. Leisure*, 844 F.2d 1347, 1354 (8th Cir. 1988). Probable cause for the issuance of a wiretap is evaluated under the same standard used to evaluate probable cause for the issuance of a search warrant. *Fairchild*, 189 F.3d at 775. Specifically, probable cause is present if the totality of the circumstances reveals that there is a fair probability that a wiretap will uncover evidence of a crime. *Id.*; *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

A magistrate judge's authority to issue a search warrant is determined by both Fed. R. Crim. P. 41(b) and 28 U.S.C. § 636. Fed. R. Crim. P. 41(b) provides that a "magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Fed. R. Crim. P. 41(b)(2). Also, "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a

tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). Section 636(a) of the Federal Magistrates Act establishes jurisdictional limitations on a magistrate judge and provides, in relevant part:

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> (1) all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts[.]

28 U.S.C. § 636(a)(1). A court's analysis of whether a NIT warrant is statutorily permissible and whether it is allowed under Rule 41(b) are necessarily intertwined. *Levin*, — F.Supp.3d at ——, 2016 WL 2596010, at *3. Indeed, "[f]or the magistrate judge to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41 (b)." *Id.* at —— n. 11, 2016 WL 2596010, at *8 n. 11.

Historically, statutory approaches have provided one mechanism for safeguarding privacy interests while, at the same time, addressing the needs of law enforcement in the face of technological change. *United States v. Ganias*, 2016 WL 3031285, at *15 (2d Cir. 2016) (en banc) (describing the enactment the then-Omnibus Crime Control and Safe Streets of Act of 1967 as a Congressional attempt to respond to and synthesize technological change, ineffective or unclear state statutory regimes, evolving Supreme Court precedent, and law enforcement concerns)

IV. DISCUSSION

Although the issues of whether the NIT constitutes a search and the defendant's standing—in terms of whether he has a legitimate privacy interest in his IP address—are back in play by virtue of the government's withdrawal of its stipulation, the court finds that it need not address those issues in light of its findings. The court finds no violation of Fed. R. Crim. P. 41 under the circumstances of this case. Even if the defendant could show a technical violation of the Rule, he has not shown a Constitutional violation so as to entitle him to suppression of the evidence. The court finds the combined conduct of the United States District Judge and magistrate judge in issuing orders that authorized interception of electronic communications and deployment of a network investigative technique in this action was authorized and allowed.

The court finds that the magistrate judge's issuance of the NIT warrant was proper in this case. Rule 41(b)(4) authorizes the magistrate judge to issue a warrant such as the NIT warrant issued in this case. That provision authorizes the use of a tracking device and the NIT is analogous to a tracking device. The NIT enabled the government to determine the website user's locations by installing a tracking device on each user's computer when that computer in essence travelled into the district of Nebraska to communicate with the website located in Nebraska. The tracking device must be installed in the magistrate judge's district, but the "warrant may authorize the

use of the device to track the movement of a person or property located within the district, outside the district or both." Fed. R. Crim. P. 41(b)(4).

The record shows the NIT warrant was issued by a U.S. Magistrate Judge within the District of Nebraska—the location of the website on which the NIT was deployed, the location into which District the users of the website communicated, and the location in which the NIT results were collected. The information obtained via the NIT—an IP address—is the same sort of information obtained in a pen register. The court finds the magistrate judge complied with Fed. R. Crim. P. 41 in issuing the warrant and his actions did not contravene 28 U.S.C. § 636 because he exercised authority that was conferred or imposed by the Federal Rules.

The warrant was issued based on probable cause established pursuant to a wiretap authorization issued by Chief Judge Laurie Smith Camp. The court's conclusion is bolstered by the fact that the probable cause for the issuance of the NIT warrant originated in orders issued pursuant to the authority conferred on the district court under 18 U.S.C. § 2561. The record shows that a district court judge approved electronic surveillance that formed the basis for the installation of the NIT warrant. By its nature, an electronic communication travels both to and from different locations and can be said to reside there for some period of time, even if that period of time is instantaneous. The court has reviewed the affidavits underlying the issuance of both the intercept orders and the NIT authorization warrants and finds they demonstrate probable cause to

believe that the electronic surveillance and the deployment of a network investigative technique would reveal evidence of the child pornography crimes at issue.

Because the magistrate judge acted within his authority and complied with Fed. R. Crim. P. 41, the court need not address whether suppression would be an appropriate remedy for a violation. Accordingly,

IT IS ORDERED:

1. Defendant's objection to the government's withdrawal of a stipulation on standing (Filing No. 558) is overruled;

2. The defendant's motion for reconsideration (Filing No. 552) is granted;

3. On reconsideration, the defendant's motion to suppress with respect to the NIT warrant (Filing No. 196) is denied.

Dated this 5th day of August, 2016.

BY THE COURT:

s/ Joseph F. Bataillon
Senior United States District Judge